UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/640,465	08/15/2000	Radia J. Perlman	SUN-P5012-RSH	4032

22835 7590 07/13/2004

PARK, VAUGHAN & FLEMING LLP
508 SECOND STREET
SUITE 201
DAVIS, CA 95616

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	6

DATE MAILED: 07/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/640,465	PERLMAN, RADIA J.	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) *2,8,14 and 21* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-7,9-13,15-20 and 22-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detailed Action

1. This action is responsive to communication: amendment filed on 12 April 2004, the original application was filed on 15 August 2000.

2. Claims 2, 8, 14, and 21 are cancelled by the amendment.

3. Claims 1, 3-7, 9-13, 15-20, and 22-26 are currently pending in this application. Claims 1, 7, 13, 19, 20, and 26 are independent claims.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claims 1, 3, 4, 5, 7, 9, 10, 11, 13, 14, 15, 16, 17, 19, 20, 22, 23, 24, and 26 are rejected under 35 U.S.C. 102(a) as being anticipated by Aziz U.S Patent No. 6,026,167 (hereinafter '167).

As to independent claim 1, "A method for facilitating a key exchange that operates with a pre-shared secret key and that hides identities of parties involved in the key exchange, comprising: initially establishing a negotiated secret key between a first party and a second party by

performing communications between the first party and the second party across a network; wherein the communications between the first party and the second party do not allow an eavesdropper to determine the negotiated secret key; encrypting an identifier for the first party using a first key that is a function of a group secret key and the negotiated secret key to form an encrypted identifier wherein the group secret key is known to members of a group, including the first party and the second party, but is kept secret from parties outside of the group" is taught in '167 col. 8, line 21-64;

"sending the encrypted identifier from the first party across the network to the second party; allowing the second party to decrypt the encrypted identifier by using the group secret key and the negotiated secret key; allowing the second party to use the identifier to look up the pre-shared secret key that was previously established between the first party and the second party; and using the pre-shared secret key in forming at least one subsequent communication between the first party and the second party" is taught in '167 col. 3 lines 7-59.

As to dependent claim 3, "wherein establishing the negotiated secret key involves using the Diffie-Hellman method to establish the negotiated secret key" is shown in '167 col. 8 lines, 21-25.

As to dependent claim 4, "wherein the second party is a firewall through which the first party seeks to communicate" is disclosed in '167 col. 7 lines 10-15.

As to dependent claim 5, "wherein the first party is a person seeking to communicate through the firewall from one of a number of possible Internet Protocol (IP) addresses" is disclosed in '167 col. col. 7 lines 10-15.

As to independent claim 7, these claims incorporate substantially similar subject matter as in cited in the claim 1 above and is rejected along the same rationale.

As to independent claims 13 and 19, these claims are directed to computer-readable storage medium of the method of claim 1 and are similarly rejected along the same rationale.

As to independent claims 20 and 26, these claims are directed to the apparatus of the method of claim 1 and are similarly rejected along the same rationale.

As to dependent claim 9-11, 15-17, and 22-24 these claims incorporate substantially similar subject matter as in cited in the claims 3-5 above and are rejected along the same rationale.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 6, 12, 18, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over '167 in further view of Tatebayashi et al., U.S. Patent No. 6,151,394 (hereinafter '394).

As to dependent claim 6, the following is not taught in '167: **"wherein the group secret key is one of a plurality of group secret keys maintained by the group"** however '394 teaches "and a plurality of reception apparatuses that are classified in to a plurality of groups, with at least two out of a plurality of secret keys being exclusively distributed to each of the groups" in col. 1, lines 60-63.

It would have been obvious to one of ordinary skill in the art at the time of the invention to the key exchange method taught in '167 to include compensation for a plurality of shared secret group keys. One of ordinary skill in the art would have been motivated to perform such a modification because it would lower the damage to a group when a shared keyed is leaked see '394 (see col. 1, lines 51 et seq.) "In view of the stated problems, it is an object of the present invention to provide an encrypted communication system that makes it difficult for third parties to decode a secret key and that limits the damage caused to the system when a secret key is leaked".

As to dependent claim 12, 18, and 25 these claims incorporate substantially similar subject matter as in cited in the claim 6 above and are rejected along the same rationale.

Response to Arguments

8. Applicant's arguments filed 12 April 2004 have been fully considered but they are not persuasive.

In response to applicant's argument on page 12, "that Aziz teaches utilizing a group interchange key ... In contrast, the instant application discloses a key exchange system that uses three keys including (1) a negotiated secret key, (2) a group secret key, and (3) a pre-shared secret key ... (1) obtained by Diffie-Hellman ... (2) ... maintained by the group through a separate mechanism ... (3) each user within the group has its own pre-shared secret key". The office states:

(1) a negotiated secret key obtained by Diffie-Hellman is the same as the public key also establish by Diffie-Hellman in Aziz col. 8, lines 21-29;

(2) the group secret key that is maintained by the group by a separate mechanism is the same as the group key utilizing the SKIP scheme which is the separate mechanism N is incremented with each communication between parties or nodes I and J.

(3) a pre-shared secret key that each user within the group has its own pre-shared key is the same as the secret value i or j shown in Aziz col. 8, lines 54-60;

In response to applicants argument on starting on page 12, 'The present invention encrypts an identifier for the first party using both the negotiated secret key and the group secret key ... is in contrast to Aziz that uses only a single key' The office disagrees Aziz teaches the pre-shared secret key or identifier for each

user (i and j) is used to calculate the shared secret key ^{ij} mod p see Aziz col. 8, lines 53-63. Note using the two identifiers is the same as utilizing two keys.

In response to applicants argument on page 13, "Additionally, the instant application discloses the decrypted identifier is used to look up a third key" the office disagrees Aziz uses the decrypted identifier as well as the number of communications between the two parties to establish a third key, instead of looking up the value in a table the Aziz calculates the values, (calculate same as lookup) in that the calculated values could also be placed into a table.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5484.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Ellen Tran
Patent Examiner
Technology Center 2134
30 June 2004